

## Personal Information Processing Agreement

This agreement is dated: [DATE] (the “**Effective Date**”).

### PARTIES

(1) [CUSTOMER], [a/an] [[PROVINCE OF ORGANIZATION]/"Canadian"] [TYPE OF ENTITY], with offices located at [registered office address] (the “**Customer**”).

(2) ASAP CHEQUES, FORMS & SUPPLIES INC., a Canadian corporation with offices located at 100 Garden Street, Gananoque, Ontario, K7G 1H9 (the “**Provider**”).

(Customer and Provider may be referred to as a “**Party**”, or collectively, the “**Parties**”).

### RECITALS

WHEREAS, the Customer and the Provider entered into the services letter agreement dated [date] (the “**Master Agreement**”) that will require the Provider to process personal information provided by or collected on behalf of the Customer; and

WHEREAS, this personal information processing agreement (the “**Processing Agreement**”) sets out additional terms, requirements and conditions for collecting, processing, disclosing, transferring or storing Personal Information when the Provider provides cheque printing services under the Master Agreement;

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Definitions and Interpretation.

1.1 The following definitions and rules of interpretation apply in this Processing Agreement.

**“Authorized Persons”** means the persons or categories of persons that the Customer authorizes to give the Provider personal information processing instructions, as identified in Appendix A.

**“Business Purpose”** means the services described in the Master Agreement and any other purpose specifically identified in Appendix A.

**“Data Subject”** means an individual who is the subject of Personal Information.

**“Personal Information”** means any information the Provider collects, processes or maintains for the Customer that: (i) relates to an individual person and identifies or can be used to identify, locate or contact that individual, either alone or when combined with other personal or identifying information that is or can be associated with that specific individual, including but not limited to: (a) first and last name; (b) home or other physical address, including street name and name of city or town and/or province or territory; (c) email address or other online information, such as a user name and password; (d) telephone number; (e) government-issued identification or other number; (f) financial or payment card account number; (g) date of birth; and (h) any information that is combined with any of (a) through (g) above; or (ii) the relevant Privacy and Data Protection Requirements otherwise defined as protected personal information.

**“Processing, processes or process”** means any activity that involves the use of Personal Information or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes or process. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Information to third parties.

**“Privacy and Data Protection Requirements”** means all applicable federal and provincial laws and regulations relating to the processing, protection or privacy of the Personal Information, including, where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

**“Security Breach”** means any act or omission that compromises the security, confidentiality, or integrity of Personal Information, or the physical, technical, administrative or organizational safeguards put in place to protect it, that rises to the level of a security breach under the Privacy and Data Protection Requirements.

**“Security Breach Contacts”** means the persons or categories of persons that each Party shall require the other Party to notify in the event of a Security Breach, as identified in Appendix A.

1.2 This Processing Agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms in the Master Agreement apply to the interpretation of this Processing Agreement.

1.3 The Appendices form part of this Processing Agreement and will have effect as if set out in full in the body of this Processing Agreement. Any reference to this Processing Agreement includes the Appendices.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Processing Agreement and any provision contained in the Appendices, the provision in the body of this Processing Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Processing Agreement or any provision contained in the Appendices, the provision contained in the Appendices will prevail;

(c) any of the provisions of this Processing Agreement and the provisions of the Master Agreement, the provisions of this Processing Agreement will prevail; and

(d) any of the provisions of this Processing Agreement and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

## 2. Personal Information Types and Processing Purposes.

2.1 The Customer retains control of the Personal Information and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

2.2 Appendix A describes the general Personal Information categories and Data Subject types the Provider may process to fulfill the Business Purposes of the Master Agreement.

## 3. Provider's Obligations.

3.1 The Provider will only process the Personal Information to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions from Authorized Persons. The Provider will not process the Personal Information for any other purpose or in a way that does not comply with this Processing Agreement or the Privacy and Data Protection Requirements. The Provider will notify the Customer if, in its opinion, the Customer's instruction would not comply with the Privacy and Data Protection Requirements.

3.2 The Provider will comply with any Customer request or instruction from Authorized Persons requiring the Provider to amend, transfer or render unusable the Personal Information, or to stop or mitigate any unauthorized processing.

3.3 The Provider will maintain the confidentiality of all Personal Information and will not disclose Personal Information to third parties unless the Customer or this Processing Agreement specifically authorizes the disclosure in compliance with Privacy and Data Protection Requirements, or as otherwise required by law. If a law requires the Provider to process or disclose Personal Information, the Provider will first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Privacy and Data Protection Requirements, considering the nature of the Provider's processing and the information available to the Provider.

3.5 The Provider will notify the Customer of any changes to Privacy and Data Protection Requirements that may adversely affect the Provider's performance of the Master Agreement.

3.6 The Customer acknowledges that the Provider is under no duty to investigate the completeness, accuracy or sufficiency of any specific Customer instructions from Authorized Persons or the Personal Information other than as required under the Privacy and Data Protection Requirements.

3.7 The Provider will be responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements.

#### 4. Provider's Employees and Contractors.

4.1 The Provider will limit Personal Information access to:

- (a) those employees and contractors who require Personal Information access to meet the Provider's obligations under this Processing Agreement and the Master Agreement; and
- (b) the part or parts of the Personal Information that those employees or contractors strictly require for the performance of their duties.

4.2 The Provider will ensure that all employees and contractors:

- (a) are informed of the Personal Information's confidential nature and use restrictions;
- (b) have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties; and
- (c) are aware both of the Provider's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this Processing Agreement.

4.3 The Provider will take commercially reasonable steps to ensure the reliability, integrity and trustworthiness of all of the Provider's employees and contractors with access to the Personal Information.

#### 5. Security.

5.1 The Provider will at all times implement appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display or distribution, and against accidental loss, destruction or damage.

5.2 The Provider will promptly notify the Customer if it becomes aware of any advance in technology and methods of working, which indicate that the Parties should adjust their security measures.

5.3 The Provider will take reasonable precautions to preserve the integrity of any Personal Information it processes and to prevent any corruption or loss of the Personal Information, including but not limited to establishing effective back-up and data restoration procedures in compliance with Privacy and Data Protection Requirements or other applicable laws.

## 6. Security Breaches and Personal Information Loss.

6.1 The Provider will promptly notify the Customer if any Personal Information is lost or destroyed or becomes damaged, corrupted or unusable.

6.2 If a Party determines there has been any Security Breach (the “**Affected Party**”), it will within ninety (90) minutes notify the other Party by contacting all of the other Party’s Security Breach Contacts identified in Appendix A and will make commercially reasonable efforts to confirm receipt of such notice by such Security Breach Contacts as soon as practicable.

6.3 Immediately following any unauthorized or unlawful Personal Information processing or Security Breach, the Parties will co-ordinate with each other to investigate the matter. The Affected Party will reasonably co-operate with the other Party in the handling of the matter, including:

- (a) assisting with any investigation;

- (b) facilitating interviews with employees, former employees and others involved in the matter; and

- (c) making available all relevant records, logs, files, data reporting and other materials required to comply with all Privacy and Data Protection Requirements or as otherwise reasonably required by the Parties.

6.4 Neither Party will inform any third party of any Security Breach without first obtaining the other Party's prior written consent, except when Privacy and Data Protection Requirements, or other laws or regulations, require it.

6.5 The Affected Party will cover all reasonable expenses associated with the performance of the obligations under Section 6.3, unless the matter arose from the other Party's specific instructions, negligence, willful default, breach of Privacy and Data Protection Requirements, or breach of this Processing Agreement, in which case the other Party will cover all reasonable expenses.

6.6 The Affected Party will also reimburse the other Party for actual reasonable expenses the other Party incurs when responding to and mitigating damages, to the extent that the Affected Party caused a Security Breach.

6.7 The Parties will maintain records of any Security Breach in accordance with Privacy and Data Protection Requirements.

## 7. Cross-Border Personal Information Transfers.

7.1 If the Privacy and Data Protection Requirements restrict cross-border Personal Information transfers, the Customer will only transfer Personal Information to the Provider under the following conditions:

- (a) the Provider, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, may legally receive that Personal Information, however, the Provider will promptly inform the Customer of any change to that status; or

- (b) the Customer obtained valid Data Subject consent to the transfer under the Privacy and Data Protection Requirements.

7.2 The Provider will not transfer any Personal Information to another country unless the transfer complies with the Privacy and Data Protection Requirements.

## 8. Subcontractors.

8.1 The Provider may only authorize a third party (subcontractor) to process the Personal Information if the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Processing Agreement and, upon the Customer's written request, provides the Customer with copies of such contracts.

8.2 Where a subcontractor fails to fulfill its obligations under such written agreement, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.3 The Provider is deemed to control any Personal Information that is controlled by or in the possession of its subcontractors.

## 9. Complaints, Data-Subject Requests and Third-Party Rights.

9.1 The Provider will promptly notify the Customer if it receives any complaint, notice, or communication that directly or indirectly relates to the Personal Information processing or to either Party's compliance with the Privacy and Data Protection Requirements.

9.2 The Provider will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.3 The Provider will not disclose the Personal Information to any Data Subject or to a third party unless the disclosure is either at the Customer's request or instruction, permitted by this Processing Agreement, or is otherwise required by the Privacy and Data Protection Requirements or other law, *provided* the Customer has been first informed of such requirement.

## 10. Term and Termination.

10.1 This Processing Agreement will remain in full force and effect until the later of the following:

(a) the Master Agreement terminates; or

(b) the Provider no longer retains any Personal Information related to the Master Agreement in its possession or control (the "**Term**").



10.2 Any provision of this Processing Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement to protect Personal Information will remain in full force and effect.

10.3 The Provider's failure to comply with the terms of this Processing Agreement is a material breach of the Master Agreement. In such event, the Customer may terminate any part of the Master Agreement authorizing the processing of Personal Information effective immediately upon written notice to the Provider without further liability or obligation.

10.4 If a change in any Privacy and Data Protection Requirement prevents either Party from fulfilling all or part of its Master Agreement obligations, the Parties will suspend the processing of Personal Information until that processing complies with the new requirements. If the Parties are unable to bring the Personal Information processing into compliance with the Privacy and Data Protection Requirement within 180 days, they may terminate the Master Agreement upon written notice to the other Party.

## 11. Data Return and Destruction.

11.1 At the Customer's request, the Provider will give the Customer a copy of or access to the Customer's Personal Information in its possession or control in the format specified by the Customer, acting reasonably.

11.2 On termination of the Master Agreement for any reason or expiration of its term, the Provider will securely destroy or render unusable, or, if directed in writing by the Customer, return and not retain, all or any Personal Information related to this Processing Agreement in its possession or control, except for back-ups that it may retain and use for audit and data recovery purposes.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents or materials that the Provider would otherwise be required to return, destroy, or render unusable, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention and establishing a specific timeline for destruction once the retention requirement ends. The Provider may only use this retained Personal Information for the required retention reason or audit purposes.

## 12. Records.

12.1 The Provider will keep detailed, accurate and up-to-date records regarding any Personal Information processing it carries out for the Customer, including but not limited to, the access, control and security of the Personal Information, subcontractors and affiliates, the processing purposes and any other records required by the applicable Privacy and Data Protection Requirements (the “**Records**”).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider’s compliance with its obligations under this Processing Agreement.

12.3 The Customer and the Provider will review the information listed in the Appendices to this Processing Agreement once a year to confirm its current accuracy and update it when required to reflect current practices.

### 13. Review.

13.1 At least once per year, the Provider will conduct reviews of its Personal Information processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Processing Agreement, including performing a network-level vulnerability assessment.

### 14. Representations and Warranties.

14.1 The Provider represents and warrants that:

- (a) it and its employees, subcontractors, agents, and any other person or persons accessing Personal Information on its behalf are professional and have received training on the Privacy and Data Protection Requirements;
- (b) it and anyone operating on its behalf will process the Personal Information in compliance with both the terms of this Processing Agreement and all applicable Privacy and Data Protection Requirements and any other applicable laws, enactments, regulations, codes, orders, standards and other similar instruments;
- (c) it has no reason to believe that any Privacy and Data Protection Requirements prevent it from providing any of the Master Agreement’s contracted services or the services hereunder; and

(d) considering the current technology environment and implementation costs, it will take commercially reasonable technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Information and the accidental loss or destruction of, or damage to, Personal Information, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage;

(ii) the nature of the Personal Information protected; and

(iii) comply with all applicable Privacy and Data Protection Requirements and its information and security policies, including the security measures required in Section 5.1.

14.2 The Customer represents and warrants that:

(a) the Provider's expected use of the Personal Information for the Business Purpose and as specifically instructed by the Customer under this Processing Agreement will comply with all Privacy and Data Protection Requirements; and

(b) the Customer will only collect Personal Information for the Provider using a notice or method that the Provider pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of the purpose or purposes for which their Personal Information will be processed by the Provider, and any other information that is required by applicable Privacy and Data Protection Requirements.

## 15. Indemnification.

15.1 Subject to Section 16, each Party (in this Section 15, the "**Indemnifying Party**") agrees to indemnify and hold harmless the other Party (in this Section 15, the "**Indemnified Party**") against all material and reasonable third-party claims incurred by the Indemnified Party or for which the Indemnified Party may become liable resulting from:

(a) any failure by the Indemnifying Party or its employees, subcontractors or agents to comply with any of its obligations under this Processing Agreement or applicable Privacy and Data Protection Requirements and any other applicable laws, enactments, regulations, codes, orders, standards and other similar instruments; or

(b) any breach of its representations warranties, covenants and other obligations under this Processing Agreement.

16. Limitation of Liability.

16.1 EXCEPT AS OTHERWISE PROVIDED IN SECTION 16.3, IN NO EVENT SHALL THE PROVIDER OR ANY OF ITS REPRESENTATIVES BE LIABLE UNDER THIS AGREEMENT TO THE CUSTOMER OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, EXEMPLARY, SPECIAL OR PUNITIVE DAMAGES WHATSOEVER, INCLUDING ANY DAMAGES FOR BUSINESS INTERRUPTION, LOSS OF USE, DATA, REVENUE OR PROFIT, COST OF CAPITAL, LOSS OF BUSINESS OPPORTUNITY, LOSS OF GOODWILL, WHETHER ARISING OUT OF BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), ANY OTHER THEORY OF LIABILITY OR OTHERWISE, REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE AND WHETHER OR NOT THE PROVIDER WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

16.2 EXCEPT AS OTHERWISE PROVIDED IN SECTION 16.3, IN NO EVENT SHALL THE PROVIDER'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING OUT OF OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EXCEED THE TOTAL AMOUNT PAID TO THE PROVIDER PURSUANT TO THE MASTER AGREEMENT IN THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM. THE FOREGOING LIMITATIONS SHALL APPLY EVEN IF THE CUSTOMER'S REMEDIES UNDER THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE.

16.3 THE LIMITATIONS SET FORTH IN SECTION 16.1 AND 16.2 SHALL NOT APPLY TO:

(a) DAMAGES OR LIABILITIES ARISING FROM THE GROSSLY NEGLIGENT ACTS OR OMISSIONS, OR WILLFUL MISCONDUCT OF THE PROVIDER IN PERFORMING ITS OBLIGATIONS UNDER THIS AGREEMENT;

(b) DAMAGES OR LIABILITIES TO THE EXTENT COVERED BY THE PROVIDER'S INSURANCE;

(c) THE PROVIDER'S OBLIGATION TO PAY LEGAL FEES AND COURT COSTS IN ACCORDANCE WITH SECTIONS 6.5 AND 6.6; OR

(d) THIRD-PARTY CLAIMS THAT ARE SUBJECT TO INDEMNIFICATION UNDER SECTION 15.

16.4 THIS SECTION 16 SETS FORTH THE PROVIDER'S SOLE LIABILITY AND ENTIRE OBLIGATION AND THE CUSTOMER'S EXCLUSIVE REMEDY FOR ANY ACTION THAT IS BROUGHT AGAINST THE PROVIDER RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

17. Insurance

17.1 During the Term, the Provider will, at its own cost and expense, obtain and maintain insurance, in full force and effect, sufficient to cover the Provider's potential indemnity or reimbursement obligations. The Provider will produce the policy and premium payment receipt to the Customer on request. The Provider will give the Customer thirty (30) days advance written notice if the policy materially changes or is cancelled.

17.2 During the Term, the Customer will, at its own cost and expense, obtain and maintain cyber liability insurance policy through an insurer licensed in Canada with limits of liability acceptable to the Provider. Without limiting the foregoing, such policy shall provide for comprehensive cyber liability coverage for first and third party liability, privacy and regulatory defense and penalties, and expense coverage, with limits no less than \$2,000,000.00 per occurrence and \$4,000,000.00 in the aggregate for all claims each policy year. The Provider may at any time during the Term request evidence of this insurance in the form of a certificate of insurance or a certified copy of the policy. If such policy is determined by the Provider to be unacceptable, the Provider may require the Customer to obtain alternative insurance coverage. The Customer shall provide the requested information and form(s) within fourteen (14) days of the Provider's initial request.

18. Notice.

18.1 Any notice or other communication given to a Party under or in connection with this Processing Agreement must be in writing and delivered to:

For the Customer: [address]

[address]

Attention: [Name of Data Privacy Contact]

Email: [•]

For the Provider: 100 Garden Street  
Gananoque, ON K7G 1H9  
Attention: Les C. Cseh  
Email: vendors@ally-business-services.com

18.2 Section 18.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution. In such cases, notices must be sent to:

Customer's legal counsel: [address]  
[contact]  
[email]

Provider's legal counsel: Viner, Kennedy, Frederick, Allan & Tobias LLP  
366 King Street East, Suite 300  
Kingston, ON K7K 6Y3  
Attention: David Doyle  
Email: ddoyle@vinerkennedy.com

#### 19. Jurisdiction.

Any action or proceeding arising out of or relating to this Agreement and the Master Agreement, and all transactions contemplated hereby or thereby must be instituted in the courts of the Province of Ontario, and each party irrevocably submits to the exclusive jurisdiction of such courts in any such action or proceeding. The parties irrevocably and unconditionally waive any objection to the venue of any action or proceeding in such courts and irrevocably waive and agree not to plead or claim in any such court that any such action or proceeding brought in any such court has been brought in an inconvenient forum. Each Party agrees that a final judgment in any such action, litigation or proceeding is conclusive and may be enforced in other jurisdictions by action on the judgment or in any other manner provided by law.

IN WITNESS WHEREOF, the Parties have executed this Processing Agreement as of the Effective Date.

[CUSTOMER]

ASAP CHEQUES, FORMS &  
SUPPLIES INC.

By \_\_\_\_\_  
Name:  
Title:

By \_\_\_\_\_  
—  
Name:  
Title:

## APPENDIX A

### PERSONAL INFORMATION PROCESSING PURPOSES AND DETAILS

**Business Purposes:** Cheque printing services; Delivery of printed cheques and related products.

**Personal Information Categories:** Account Holder (including Name(s); Addresses; Bank Account Number(s); Contact Information; Bank Account Type (personal or business); Bank Account Package; Bank Branch (including Financial Institution Name and Address, MICR transit/routing).

**Data Subject Types:** Personal; Business.

**Authorized Persons:**

1. [Name]
2. [Name]

[Note: To be completed with input from the credit union Customer.] and such other Authorized Persons that are added in writing in accordance the Provider's policies.

**Security Breach Contacts:**

Provider Contacts:

[Name 1]

Email(s): [•]

Telephone Number: [•]

[Name 2]

Email(s): [•]

Telephone Number: [•]

Customer Contacts:

[Name 1]

Email(s): [•]

Telephone Number: [•]

[Name 2]

Email(s): [•]



Telephone Number: [•]

---

**END OF  
DOCUMENT**

4813-6163-6794, v. 7